REVIEW

Surveillance and Security: Protecting Electricity Utilities and other Critical Infrastructures

Antonios Gouglidis[1*], Benjamin Green[1], David Hutchison[1], Ali Alshawish[2] and Hermann de Meer[2]

*Correspondence:
a.gouglidis@lancaster.ac.uk
[1]School of Computing and Communications, Lancaster University, InfoLab21, LA1 4WA Lancaster, UK
Full list of author information is available at the end of the article

Abstract

Critical infrastructures – such as electricity networks, power stations and Smart Grids – are increasingly monitored and controlled by computing and communication technologies. The need to address security and protection of electricity infrastructures with a high priority has broadly been recognized. This is driven by many factors, including the rapid evolution of threats and consistent technological advancements of malicious actors as well as potentially catastrophic consequences of disruptions of such systems. Surveillance and security technologies are traditionally used in these contexts as a protection mechanism that maintains situational awareness and provides appropriate alerts. Surveillance is a cumbersome process because of the need to monitor a diverse set of objects, but it is absolutely essential to detect promptly the occurrence of adverse events or conditions. The aims of this paper are twofold: First, we describe two surveillance architectures in which different technologies can be used jointly for boosting the safety and security of electricity utilities and other key resources and critical infrastructures. Second, we review the typical surveillance and security technologies and evaluate them in the context of critical infrastructures, which may help in making recommendations and improvements for the future. To accomplish these aims, we extracted and consolidated information from major survey papers. This led to identifying the surveillance and security technologies, their application areas, and challenges that they face. We also investigate the perceived performance of the identified technologies in critical infrastructures. The latter comes from interviewing experts who operate in critical infrastructures, and thus provide indications for protecting critical infrastructures, not least because of their increasing use of cyber-physical elements.

Keywords: Critical infrastructures protection; cyber-physical systems; privacy; resilience; security; surveillance; utility networks

Introduction

Electricity utilities represent one of the essential (critical) infrastructures of our modern society. Almost all aspects of our modern life (e.g., communication, transportation, food, health-care) depend heavily on a reliable supply of electricity. Over the course of the last few decades, these systems have become increasingly complex, large, and interconnected. This development has been mainly driven by a variety of economic, regulatory, social, and operational factors. Operationally, the geographical expansion and the extensive interconnection of electric power distribution can play a key role in maintaining the reliability of these systems. Their ability to withstand unforeseen disturbances can be boosted by aggregating complementary loads and hence effectively having supply and demand in balance. Electricity systems

reliability is further improved by combining a large number of generation units and pooling their power reserves to collectively overcome failures and sudden outages. They are, therefore, characterized as a large-scale complex system-of-systems that encompasses basically three phases: power generation (bulk power generators, renewable energy sources), power delivery (high-voltage transmission as well as medium and low-voltage distribution), and power demand (the electrical loads). Holistic (or even subsystem-specific) control and monitoring functions, which are facilitated by the various technological advancements, play a pivotal role in the development of electricity utilities. These technologies include – to mention but a few – flexible AC transmission systems (FACTS) controllers, phasor measurement units (PMU), and advanced metering infrastructures (AMI).

While productivity, availability, quality of supply, cost, and reliability have been considered with a higher priority when designing and operating traditional electricity utilities, security and protection issues of such systems are increasingly demanding a careful attention. Cyber and physical security aim at enhancing the ability of power systems to withstand the different threats facing their assets including their data, processes, components and subsystems. These threats include, but not limited to, natural disasters, technological disasters due to human errors, deliberate or non-deliberate attacks, and terrorism. For example, in 2013, a sniper attack at PG&E Corp.'s Metcalf transmission substation knocked out 17 giant transformers and the workers struggled for 27 days to recover [1]. Due to the extensive adoption of Information and Communication Technologies (ICT) in electric power system's operations, they are not only vulnerable to physical attacks but also to cyber-attacks that were previously only common in IT security. The cyber-physical nature of power systems opens the door for potential attackers to cause a serious physical damage from a remote location and without any physical presence in the target facility. In December 2015, external cyber-attackers launched a synchronized and coordinated cyber-attack on Ukrainian power companies and other organisations in variety of critical infrastructure sectors. The attack caused massive power outages impacting a large customer base in Ukraine [2]. Given the enormous scale of power systems and interdependencies with other critical infrastructures [3] has identified three basic security threats relevant to electricity infrastructures: (i) Attacks upon the power system targeting components of the power system and aiming at causing damage and loss to the victim power system in the first place. (ii) Attacks by the power system targeting the population by leveraging the power system's parts as a weapon (iii) Attacks through the power system targeting the other interconnected utility network exploiting the risk of cascading failures to cross the boundaries of interconnected infrastructures.

Therefore, the complex nature of electricity utilities and the increased rate of collaboration and interconnection renders the traditional security solutions ineffective. As a result, the assumption that the inside doesn't have risk sources and it is subsequently equipped with less protection is no more valid. On the contrary, it is highly important to maintain situational awareness even within the system boundaries so that the potential attackers can still be detected, and the security managers are able to respond proactively. Observation and monitoring activities of the various power systems' processes and subsystems are a key source of information required

for the situational awareness process in place. This process aims at understanding the current security posture of the system and further predicting future states towards getting ahead of potential attackers. The wide range of security technologies and sensors allow the monitoring of human activities as well as physical and digital assets and processes. Monitoring is an initial and crucial part of obtaining, fusing, and processing data needed for issuing immediate alarms and making informed decisions. Therefore, having dynamic surveillance systems will definitely improve the situational awareness and hence boosting the security posture of the power systems [4]. Generally speaking, security has been characterised as the dominant driver with regards to the development and deployment of surveillance solutions [5]. While our main interest is in smart grid and power facilities, the results on surveillance technologies we are presenting are generic enough to be applicable to critical infrastructures in general. Therefore, we do not talk explicitly about electricity systems in the subsequent sections of the paper.

The role of surveillance

Surveillance is mostly concerned with the monitoring, in a systematic way, of the actions or communications of one or more individuals. The collection of information with regard to individuals, their activities, or their associates is its main purpose. Another potential intention of surveillance may be to deter a whole population from undertaking some kinds of activity [6]. Currently, and traditionally, a broad range of surveillance technologies is used, across a very wide variety of scenarios [7, 8]. However, in this paper we are mostly interested in examining surveillance and security in the context of power grids and critical infrastructures (CIs) that are monitored and controlled by computing and communication technologies. Monitoring approaches are mainly used for the detection of events or actions that deviate from normal behaviour, thus, rendering surveillance an enabler for protecting systems. As argued in [9, 10], the protection of CIs is essential for the orderly functioning of a society, its economy and national sovereignty. Now, more than ever, critical infrastructures are facing an increase in the number and severity of threats [9, 11], and thus we require security systems to operate as a protective means towards the detection of actions that could result in catastrophe.

During the past few decades, security technologies have taken a significant leap forward through rapid and continuous advances in science and technologies, which have indeed played an enabling role in the process of developing security to go beyond its traditional practices, such as keeping watch over physical entities using Closed-Circuit TeleVision (CCTV) cameras, to become pervasive systems that can monitor almost all activities and transactions in both physical and cyber worlds. Before the era of the Internet, security systems tended to prevent or warn of physical trespass, harm, natural disasters or criminal actions. They are still applied in public areas, train stations, airports, stadiums, banks, and the military as well as high-security facilities and much more. Traditionally, we have deployed security solutions, such as CCTV, access control and other systems, to achieve physical security functionalities. Nowadays, cyber-attacks are increasing in number and severity. Hence, intruders need no longer trespass into facilities by using excessive, or any, physical force. Instead, they can use the Internet to gain access to companies, governmental

and public agencies, and so on. Critical data can be stolen or even manipulated. Specifically, cyber-attacks against critical infrastructures have the potential for a widespread impact on almost all sectors of our societies, and therefore terrorist organisations have shown an increasing interest in this kind of warfare. Conventional protection systems were not designed to counter cyber-attacks; therefore, new mechanisms have emerged, such as 'dataveillance', to prevent fraud, monitor activities of these sorts of attackers, etc. Concisely, security, in terms of physical and cyber manifestations, represents an integrated solution for protecting cyber-physical systems by incorporating a wide variety of technologies for perimeter or boundary monitoring, observing of human activities, and monitoring of control and operational processes. These technologies can function synergistically to overcome the limitations of each individual technology and consequently allow correlation of inputs from multiple technologies to enhance safety, security, and operational efficiency, simultaneously.

Nevertheless, despite the evolution of surveillance and security technologies and their advancements, there are no solutions, to the best of our knowledge, which are in a position to combine and match risk metrics, i.e., interconnected metrics stemming from both physical and cyber environments. Such metrics could eventually be used by computer-based surveillance solutions to keep critical infrastructures resilient. We have defined 'resilience' in [12] as the ability of a system or network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation. This definition resulted from research conducted in the EU ResumeNet project [13]. The use of such technologies in the context of a resilience strategy [14] may provide significant information in order to promptly detect the occurrence of adverse events or conditions [15] in a critical infrastructure.

Our motivation to investigate the state of the art in surveillance and security technologies stems from our intent on developing innovative systems for protecting critical infrastructures and improving their resilience. The aim is to compile an overview of current technological trends and practices, as well as evaluating them in order to identify potential gaps in technologies or ways of improving them. Although several taxonomies exist [16], a compact yet functional list of technologies that will facilitate their evaluation in the context of critical infrastructures is not evident. We anticipate that fulfilling the above mentioned aim would facilitate the interaction amongst relevant communities, e.g., critical infrastructure operators and end-users, suppliers of security products, services policy makers and research organisations [17], and encourage the development of innovative systems for protecting critical infrastructures [18].

The remainder of this paper is organised as follows: the next section introduces surveillance architectures used in critical infrastructures, electricity, power stations and Smart Grids. Subsequently, we provide the results of a systematic literature review on security technologies applicable in surveillance architectures and a comparative evaluation of the main categories. The evaluation results represent the perception of experts with regards to security technologies currently implemented in their organisation. Finally, we discuss our findings and provide concluding remarks, then indicate potential future directions.

Surveillance architectures

In this section, we introduce and describe surveillance architectures employed in critical infrastructures, specifically in utility networks, such as electricity. This information is obtained from discussions with engineers with expertise in the underlying architectures and surveillance technologies used in utility networks. We consider this to be expert knowledge – and applicable in the majority of electricity utility networks.

Based on the Purdue model in [19], we identify two main different areas of utility networks in which surveillance technologies can be applied. Specifically, these are the enterprise zone (top layers of the Purdue model) and manufacturing zone (bottom layers of the Purdue model). Concerning the enterprise zone, we assume the existence of surveillance technologies/architectures that are applicable and similar to the majority of technologies/architectures used in enterprise environments. The biggest interest for us is the manufacturing zone, which differs in several ways from the top layers of the infrastructure. In the remainder of this section, we describe in more detail two main surveillance architectures applicable in utility networks. In this paper, we correlate the size of field sites with the number of people being served by the utility provider. We also note that the types of surveillance technologies and architectures are highly dependent on the criticality of the processes taking place on a field site, i.e. we assume that simple surveillance architectures are best suited for field sites with low criticality, and more advanced architectures will be required for field sites performing highly critical processes.

Simple surveillance architectures

In this section, we provide a generic surveillance approach that may be applicable in small and/or low criticality field sites. In such cases, a suitably generic architecture of the surveillance system is illustrated in Figure 1. In this architecture, we have three main points of concern. The first consists of field sites that are under protection; second, we have the main offices of the utility network in which a supervisory system is located; and finally, there may be a third-party company which is in position to provide assistance in case of an alarm. In the following, we provide a comprehensive description of the operations that can occur in this sort of surveillance architecture.

One of the most basic component types in field sites is that of sensors. Depending on the set of equipment installed on the field site and the level of awareness that a utility provider needs to have, various types of sensors can be installed. In simple setups, sensors are mostly in position to provide bitwise information. Bitwise information is required in order to identify changes in the status of an object. An example would be the installation of binary sensors on fence gates, cabinet doors, etc., in order to check if these are open or closed. In case someone enters the field site via a fence gate, this would result in triggering the attached sensors. Other cases would include the installation of motion detection sensors to detect intruders on the field or the removal and/or alteration of field site devices. In a similar way, motion detection sensors trigger analogous alarms. In all cases, this information is conveyed to a local security box or in the absence of it, directly to a Remote Terminal Unit (RTU) located onsite. RTUs, also sometimes called Remote Telemetry Units [20],

are devices that are able to communicate with field site devices and the supervisory system (Master Terminal Unit) located within the Demilitarised Zone (DMZ) through a variety of communication systems (Radio, DSL, Satellite, etc.) [21]. The data received from local field site devices is interpreted by the RTU and then conveyed to the supervisory system, where human operators are in position to review the events that happen. Nevertheless, due to RTUs physical restrictions, e.g. a small number of input/output slots, it is required in many cases to have set in place a local security box. The latter is usually a device that is able to aggregate all the information provided by various sensors of a field site. Thus, it is able to keep track of all connected sensors, and therefore, to provide information about their status. In case of a breach, the security box is informed by the individual sensor and it subsequently sends a signal to the RTU. The latter then forwards a signal to the supervisory system in order to alert the human operators that something requires their attention.

After receiving the signal from the RTU, the human operators are in position to open a remote session with the security box (e.g., instantiate a connection using IP-based protocols). The operators, when connecting with the security box, are able to get specific information about the status of all connected sensors, and thus to further investigate the problem. An additional telephone connection between the main offices and the security box onsite provides the functionality to perform calls to the security box, which is usually equipped with microphones, thus allowing the operators to receive further audio information about the status of the remote point for increased situational awareness (e.g., hearing ambient noise). After sorting out the potential problem (e.g., people sent to the field site to check the situation) sensors are restored to their initial state. It is worth mentioning that in many cases an external third-party company that provides monitoring/surveillance services might be put in place. In the presence of this additional actor, the field site (i.e., the security box) is usually passively monitored by the third-party. Specifically, in the case of an alarm, operators of the utility provider should acknowledge within the system that they are aware of it. Since third-party providers monitor the infrastructure in parallel, they can identify whether the utility provider has acknowledged the alarm. In the absence of an acknowledgement, third-party providers can act on behalf of the utility operators and subsequently inform them about the incident.

Figure 1 Simple surveillance architecture for utility networks.

Advanced surveillance architectures

Although the architecture presented in the previous section consist of a simple and inexpensive solution for typical small-scale field sites, it fails to scale up and to cope with larger field sites where highly critical processes are in place. In order to support these large field sites, with a greater number and variety of sensors as well as higher criticality, this requires a more advanced set of software and hardware solutions. Usually, third-party companies provide such solutions by providing integrated systems for controlling and monitoring the underlying critical infrastructure.

In general, these advanced settings are capable of integrating information from a wide range of sensors, including cameras, points of access control, field site perimeter, etc. All information stemming from the individual sensors in a field site is collected on a local data server (see Figure 2). Thus, local client systems are able to access this information and receive a wide range of indications. These systems typically provide a suitable graphical user interface to facilitate the process of getting notified by alarms and to help operators to identify root causes of problems.

In the presence of an incident, the local data server logs an alarm triggered by one or more of the sensors. This information is subsequently conveyed to the local client system. The latter provides visual warnings to human operators (e.g., building identification through blinking) to highlight the alarm via a sophisticated graphical user interface. This consist of level one map in a series of three. In turn, operators are able to further zoom in to the area/building by agreeing to investigate the triggered alarm. The last phase includes further zooming in to the building and getting fine-grained information about the place of the incident (e.g., floor and/or room). Operations and functionality provided at this level of interaction with the graphical user interface include access to remote devices as cameras for a live view of the area, etc.

This is a process that can be replicated in all individual field sites of a utility provider. Hence, in case of large service providers, this information can be further scaled up via having a central office where an overall status view of all connected field sites is provided (e.g., country level map). Thus, in this case, alarms are conveyed from various local data servers to the main by attaching also the functionality to zoom in to individual alarms remotely.

Figure 2 Advanced surveillance architecture for utility networks.

Surveillance and security technologies

In this section, we list surveillance and security technologies as identified in the existing literature and may be applicable in surveillance architectures as the ones described in the 'Surveillance architectures' Section. The retrieval of technologies was carried out from manuscripts that were obtained from several on-line electronic databases. Specifically, to cover the majority of existing technologies, information was retrieved from major survey papers. The examination of collected material resulted in the identification of six main types of technologies based on their offered functionality. Although a strict categorisation may be cumbersome – many technologies can be partially used in more than one area for the implemented devices to provide the desired level of functionality – we have identified the following main types, viz. biometrics, dataveillance, visual surveillance, communication surveillance, location tracking, and ubiquitous surveillance. The individual technologies and techniques within each of the categories listed in Table 1 may offer a different functionality (e.g., identification, detection, verification) to fulfil different security requirements (e.g., access control, cyber security, perimeter protection [16].

In addition to the list of identified technologies, we include in Table 2 a series of sensors and transducers that could operate in more than one of the technologies

identified in Table 1. The reason for separating the set of sensors/transducers from the list of technologies is that the former can be used by a variety of surveillance and security technologies. The sole application of any sensor/transducer does not result in having a surveillance or security technology on its own.

In the following, we provide brief details about the identified types of surveillance and security technologies; of course, more information concerning each of the technologies can be retrieved from the individual documents.

Table 1 List of surveillance and security technologies.

Type	Technologies	Examples of techniques or devices per technology
Visual surveillance	Video	Smart CCTV
[22, 23, 24, 25, 26, 27, 28, 7]	Imaging scanner	Infrared scanners, sonar imaging, thermal imaging, x-ray imaging, radiation imaging
	Photography	Cameras, mobile phones, mobile video
	UAVs	Drones, balloons
Biometrics	Physiological	Face recognition, facial thermograph, fingerprint recognition, retina scanning
[22, 23, 25, 29, 30]	Behavioural	Infrared scanners, sonar imaging, thermal imaging, x-ray imaging, radiation imaging
	Multimodal biometrics	Multiple biometrics, multi-algorithm systems, multi-sensor systems
Communication surveillance	Cyber security	Voice over IP, mobile phones, call logging
[22, 23, 24]	Physical	Wiretapping
Location tracking	Proximity sensing	Proximity sensors
[22, 23, 24, 7]	Scene analysis	Image recognition algorithms
	Triangulation	Triangulation algorithms
Dataveillance	Cyber security	Intrusion detection and prevention systems, anti-malware, deep packet inspection
[22, 23, 29, 31]	Data analysis	Data mining and profiling
	Triangulation	Triangulation algorithms
Ubiquitous surveillance	Embedded sensors	Wearable digital media
[7, 32]		

Table 2 List of sensors/transducers.

Sensors/Transducers [22, 23, 24, 25, 33, 34]
Audio and acoustic sensors
Binary sensors
Explosives detector
Radio frequency identification (RFID)
Gas chromatography mass spectrometry detector
Heat sensors
Infrared sensors
Metal detectors
Microwave sensors
Radar sensors
Under sea detectors
X-rays detectors

Visual surveillance

Technologies: Visual surveillance includes a very wide variety of technologies. The main technology categories identified in the examined literature include those of video, imaging scanners, photography and Unmanned Aerial Vehicles (UAVs). Visual surveillance is mentioned in [35] to equate with the supervision, close observation, and invigilation of individuals who are not trusted to work or go about unwatched.

Application areas: Visual surveillance systems are closely coupled 'with the concept of territorial privacy; that is, the fact that our assumption of privacy varies with place' [36]. When it involves people or vehicles, surveillance applications may be used for 'access control in special areas; person-specific identification in certain scenes; crowd flux statistics and congestion analysis; anomaly detection and alarming; and, interactive surveillance using multiple cameras' [37, 38]. Therefore, application areas for video surveillance could be the protection of private properties/workplaces (e.g., employee monitoring), border or perimeter control, public spaces (e.g., banks, schools, transport systems, etc.), monitoring for criminal and anti-social behaviour etc. Similarly, photography technologies are applicable in areas such as the identification and monitoring of both public and private spaces (e.g., surveillance of suspects or known criminals, passport holders and car drivers by the police, filming accidents etc.) [24]. In turn, UAVs (drones) are mostly used in military operations, policing, border or perimeter control, emergency response and monitoring for environmental hazards.

Challenges: Visual surveillance deals with various challenges including those of privacy centric challenges [29], technical issues (e.g., systems integration), and/or related to algorithmic problems (e.g., 3-D tracking, behavioural understanding) [37]. In addition, in some cases the operating environment of a device (e.g., level of light and ambient conditions), or even the positioning of it [29] could be a significant challenge.

Biometrics

Technologies: Biometric technologies refer to automated methods that are able to identify or recognise the identity of a living person, after analysing some of his/her characteristics (e.g., physiological and/or behavioural characteristics) [39, 40]. Examples of biometric technologies that consider the physiological characteristics of a person are these of face recognition, facial thermogram, recognition of fingerprints, the geometry of hands, iris or retina scanning, etc. In addition, behavioural oriented biometric technologies include those that can recognise someone's manner of walking (i.e., gait recognition), analyse the way people type using a keyboard (i.e., keystroke analysis), how they operate a pointing device (e.g., mouse dynamics in the case of a mouse), signature analysis, or even performing a waveform analysis of people's voices to verify their identity. Finally, another category of biometrics is that of multimodal biometric systems, which refer to systems that include multiple sources in order to establish the identity of an individual [41].

Application areas: The main objective of biometric technologies is to identify, verify, or authorise an individual. That objective is mainly accomplished through the application of pattern-matching algorithms on a set of collected data (usually kept in database systems). Therefore, some of the domains in which biometric technologies find a use are systems applicable to immigration and border control (e.g., use of biometric 'chipped' passports [42]); to criminal justice systems and profiling systems (e.g., the Combined DNA Index System (CODIS) [43] used by the FBI and U.S. Department of Justice); national identity systems, etc. [23]. Despite the wide spectrum of applications of biometric technologies, their capabilities are mostly restricted to the monitoring of people through identification or verification operations.

Challenges: Despite the high effectiveness of biometric technologies, there are recognised challenges that should be considered when using them. In most of the examined studies, security and privacy concerns are identified as key challenges. Another interesting challenge is that of the reliability level offered by biometric technologies (e.g., reliability with regard to DNA comparison), or even vulnerabilities that might exist in a system operating with biometric technologies [44].

Communication surveillance

Technologies: Communication surveillance can be defined as the 'monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communication networks to a group of recipients by a third party' [1]. When compared with dataveillance, communication surveillance is mostly about voice call surveillance.

Application areas: This sort of technology has a level of ambiguity, connected with the reason for using it, e.g., the use of communication surveillance to protect nations against terrorism. On the contrary, since such technology is strongly linked with the notion of electronic eavesdropping it could be perceived as a tool for conducting espionage [45].

Challenges: Representative challenges in communication surveillance include how to overcome the issues of human rights violation to privacy and freedom of expression. It is worth noting that despite the fact that all security technologies infringe individuals' privacy, in the case of communications surveillance the breadth and depth of privacy infringement is usually difficult to foresee [45, 46].

Location tracking

Technologies: The main set of technologies used to perform tracking of locations could be summarised into three main categories, viz. proximity sensing, scene analysis, and triangulation [23, 47]. Proximity sensing refers to the ability of a sensor to identify if it is near to an object, and/or to be able to measure that distance (depending on the complexity of the sensor)[2]. Scene analysis refers to systems that are able to infer an entity's/object's position from a neighbouring relation (e.g., via the use image recognition algorithms) [23]. Finally, triangulation is a method for the determination of an entity's/object's location or distance to a point by measuring two fixed angles [3].

Application areas: Location tracking has a broad range of application areas including global positioning systems (GPS) for the determination of an entity/object, and determination of the spatial dimensions and geometry of objects. Such technologies appear to be useful in military operations, espionage or policing.

Challenges: The main value of location tracking technologies could also be one of its biggest concerns as well. The potential to leak some information about a person's location, if this is not desirable, may lead eventually to privacy infringement. Along with privacy issues, other types of challenge are technical ones, e.g., assuming a sanitizer 'given a video, a sanitization request, and access to the location database'

[1] https://www.privacyinternational.org/
[2] https://whatis.techtarget.com/definition/proximity-sensing
[3] https://en.wikipedia.org/wiki/Triangulation

to 'jointly satisfy the privacy objective of the surveilled while preserving the image dissemination objective of the surveiller' as described in [36].

Dataveillance

Technologies: In [6] Clarke defines dataveillance as the 'systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons'. As stated in [23], the term dataveillance usually appears in the literature as the trend of applying security practices on personal data, and regulates or governs people's behaviour [48]. Such security practices may include electronic processing of data, which will eventually result in providing an adequate level of security. Technologies used in dataveillance systems include those of intrusion detection, prevention and deep-packet inspection systems [49] for cyber security. There are also cases where honeypot, honey-spam and anti-malware systems are set in place, usually having a defensive character. Additionally, data analysis makes use of several technologies, namely data integration (e.g., data marts and data warehouses) [50, 51], virtual machine introspection [52], and database and data retention systems. The latter refer to the definition of a set of policies on persistence and management of data for meeting specific legal and business data archival requirements [4].

Application areas: One important application area for dataveillance technologies is their use by security agencies and bodies to perform pattern recognition and predictions [23]. Such approaches usually depend on the use of data-mining techniques. Other technologies used in data processing techniques include pattern recognition and prediction. Dataveillance technologies could be also used by employers to monitor employees (monitoring of calls, e-mails, or even computer keystrokes); used in targeted environments or even mass surveillance (e.g., profiling via data mining); apply deep packet analysis to detect, block and protect against security threats, enforce parental control; or even to prevent exfiltration of private or classified information.

Challenges: The key challenges in dataveillance vary from technological [53] to legislation [54] (e.g., privacy issues). More specific examples with regard to technological challenges, and mostly related to cyber security and deep packet inspection, include capturing and processing of packets in multi-gigabit links without any packet loss; the existence of a large number of application signatures and their complexity; and the potential unpredictability imposed by network flows or packet payloads with regard to their signatures, which could eventually lead to a degraded performance of Deep Packet Inspection (DPI) services [55].

Ubiquitous surveillance

Technologies: Ubiquitous surveillance are related to the unilateral gathering of data on people in their living environment, through the use of various embedded sensors [56]. Some generic categories of technologies are these of ICT implants, the use of smartphones, and that of wearable digital media (e.g., cameras, microphones, etc.).

Application areas: The application areas of ubiquitous surveillance and computing devices are numerous since they are applicable almost everywhere, i.e., applicable

[4] https://en.wikipedia.org/wiki/Data_retention

to any type of objects (e.g., clothing), on people, and even in places [57]. Interesting application areas of ubiquitous surveillance could be data recording (e.g., used to augment human memory through passive recording of images), localisation/tracking of people (in collaboration with location tracking technologies), identification of people (in collaboration with biometric technologies), or even the provision of personal protection services in combination with other technologies.

Challenges: One of the biggest issues with regards to ubiquitous surveillance and computing is privacy. This is mainly the result of the seamless integration and pervasiveness of ubiquitous technologies in almost all types of environment [58], and because they may potentially lead to or are prone to information leakage [59].

Comparative Evaluation of Technologies

In this section, we provide a comparative evaluation of the examined type of identified technologies based on six metrics, viz. security, privacy, usability, effectiveness, cost, and cost effectiveness. The defined metrics are examined using a qualitative scale (see Appendix B). Specifically, we examined the above metrics in the following context:

Security – Provides an average perception of the efficiency of a technology to detect security violations.

Privacy – Provides an average perception of the level of privacy infringement imposed by a security technology, and the examination of the concept of privacy-by-design (as examined in [23]). Nevertheless, the evaluation of both properties is not a straightforward process and is based on the experience and the perception of the evaluator, e.g., researchers and operators. Higher values result in higher privacy infringement.

Usability – Provides an average perception of the level of simplicity, ease of use, and learnability of a security technology. Higher values are interpreted as being easier to use and/or learn how to operate a particular type of technology.

Effectiveness – Provides an average perception of the level of completeness and accuracy with which the technology achieves specific goals.

Cost – Provides an average perception of various financial costs of a security technology. This might include the cost of purchasing a device, operating costs, personnel cost, etc. Calculating cost is considered to be a challenging process and can be estimated on an hourly basis (e.g., average costs of various location tracking methods [60]). In order to cope with the cost of security technologies, we express it on the basis of a qualitative scale (see Appendix B).

Cost effectiveness – Represents the relative cost and effectiveness of security technologies. More information with regard to evaluating cost effectiveness is provided in Appendix B.

The data used for the analysis was based on the perception of experts operating in five different organisations, three of them directly involved and two indirectly involved in operating critical infrastructures; they provided their perception of each of the technologies present in their infrastructure. Our approach uses a basic qualitative research analysis. Such approach suits research problems characterised by the following: the sample size of data can be relatively small, and the interpretation of data can be based on data that reflect experts' perspective. To collect data, people in utility networks completed a table of security technologies. Specifically, they

were asked to provide their opinion on the level of security, privacy, etc., provided by each of the security technologies present in their infrastructure.

In Table 3, we provide the type of technologies that have been identified to be present in the water utility, electrical energy supplier, and the refinery. This information contributes to understand how security technologies are used per critical infrastructure. Some notable findings are that behavioural and multimodal technologies under biometrics, UAVs under visual surveillance and scene analysis techniques under location tracking are not used in the examined infrastructures. On the contrary, video technologies under visual surveillance and cyber security technologies under communication surveillance appear to be present in all three critical infrastructures. Likewise, several types of sensors are used in each infrastructure to monitor processes. Detailed information about the actual applied techniques and type of sensors is omitted due to privacy concerns.

Evaluation information is depicted in Table 4, indicating types of security technologies and the relative importance of metrics according to operators' subjective perception. More information on the results presented in Table 4 is provided in Appendix C.

When examining security, the analysis of data indicates three classes of security, i.e., technologies that can offer a high level of security, such as biometrics and location tracking; technologies that offer a medium level of security, such as visual surveillance, communication surveillance and dataveillance; and technologies that offer a lower level of security when compared to the rest of technologies, such as ubiquitous surveillance.

A similar pattern to security appears to be followed also by privacy infringement. Specifically, based on the perception of experts, location tracking is identified as the type that imposes the highest level of privacy infringement. The lowest value is imposed by ubiquitous and dataveillance technologies, while the rest of the examined areas are evaluated to introduce approximately the same medium-level of privacy infringement.

The level of usability appears to be equally for biometric and location tracking technologies. Visual and communication surveillance follow in the second and third positions, respectively, and dataveillance performs slightly better than ubiquitous surveillance, which provides the lowest usability level when compared with the rest of technologies (see Appendix C for detailed values).

Concerning effectiveness, biometrics and dataveillance appear to be the most effective type of security technology, while ubiquitous surveillance the least effective. The majority of the rest of the examined security technologies provide a more or less equal level of effectiveness. With regard to cost estimation, location tracking and dataveillance are the most expensive, while ubiquitous appears to be the least expensive form of security technology. The combined examination of cost and effectiveness of security technologies provides us with the potential to examine their cost effectiveness. Specifically, we see that biometrics appear to be most cost effective; ubiquitous surveillance is perceived as the least cost effective, while the remaining examined security technologies are equally cost effective.

Table 3 Surveillance and security technologies per examined critical infrastructure.

Type	Technologies	Water utility	Electricity utility	Refinery
Visual surv.	Video	X	X	X
	Imaging	X	X	
	Photography		X	
Biometrics	Physiological	X		X
Communication surv.	Cyber security	X	X	X
	Physical	X	X	X
Location tracking	Proximity sensing	X		
	Triangulation	X	X	
Dataveillance	Cyber surv.	X	X	X
	Data analysis	X	X	
Ubiquitous surv.	Embedded sensors	X	X	

Table 4 Evaluation of surveillance and security technologies based on operators' subjective perception.

	Security	Privacy	Usability	Effectiveness	Cost	Cost effectiveness
Visual surveillance	Medium	Medium	Medium	Low	Low	Low
Biometrics	High	Medium	Medium	Medium	Low	Medium
Communication surv.	Medium	Medium	Medium	Low	Low	Low
Location tracking	High	High	Medium	Low	Medium	Low
Dataveillance	Medium	Low	Low	Medium	Medium	Low
Ubiquitous surv.	Very low	Low	Low	Very low	Very low	Very low

Very high: value > 0.8, High: $0.8 \leq$ value < 0.6, Medium: $0.6 \leq$ value < 0.4,
Low: $0.4 \leq$ value < 0.2, Very low: value ≤ 0.2 (see Appendix C for values)

Discussion, Related Research, and Conclusion

A first step in our analysis was to identify the major surveillance and security technologies and to categorise them. The categorisation we applied was based on the collection of information from several research works, and this resulted in the definition of six main types (see Table 1). The definition of the main technology types served as the basis of identifying some of the emerging technologies used per se. We note that the list of technologies in each type could be more extensive.

It is interesting that the metrics we defined for performing the analysis of technologies in this survey were not extensively covered by previous research. In this paper, we include and define security based on the perception of the authors; we see this as extremely important. By contrast, privacy clearly emerges from the examined studies as the most important issue in the security landscape. Privacy was examined in several of the primary studies and under various contexts and was also identified as one of the most important future challenges in security.

With regard to the set of defined metrics (see Table 4) – some of them have been examined in similar analyses of surveillance and security technologies. However, to the best of our knowledge, an analysis of these metrics in the context of critical infrastructures was missing. Specifically, we anticipate that our analysis can provide practical information and indications about the level of security, privacy, usability and cost effectiveness provided by security technologies in utility networks. Moreover, to cope with potential controversy on the evaluation of the examined metrics, we argue that their evaluation based on a qualitative scale and incorporation of the 'confidence' metric during the collection of data have greatly amplified the completion of this task in an efficient way (see Appendix B).

To the best of our knowledge, the addressed research works appear to be the most relevant sources of information with regards to surveillance and security technologies. However, none of this representative literature appears to examine them in

the context of critical infrastructures. Additionally, apart from the research work conducted in [24] (which is restricted to a subset of technologies related to crime investigation), none of the rest referred to the evaluation of security, privacy infringement, usability, effectiveness, cost, and cost effectiveness. And none of the existing surveys included an evaluation of technologies based on the perception of experts. Specifically, the evaluation of surveillance and security technologies in the context of critical infrastructures and identification of biometrics as one of the most cost-effective technologies motivated us to further investigate the application of mobile identification checking devices with support of facial and fingertip recognition in an industrial environment [61], where following a game theoretic decision making framework we defined optimum patrol strategies [62].

The implementation of an 'open surveillance' system is an important step in realising a resilience strategy and framework for protecting critical infrastructures [9, 12]. The resulting 'open resilience' system will provide monitoring of the extended perimeter of multi-stakeholder cyber physical systems, and thus prompt detection when an adverse event or condition occurs.

Other critical infrastructures – such as Smart Grids – are evolving into complex cyber-physical systems, and therefore, ensuring their protection is considered to be a multi-variable problem. Socio-technical systems can be defined as multi-stakeholder cyber physical systems, with the latter being comprised of physical and computational resources. Surveillance can support the situational awareness in such large-scale systems through the provision of multidimensional data required to build an integrated picture of the current and future system's states. Hence, an efficient surveillance solution constructed by deployment of appropriate sensor and monitoring technologies will definitely improve the ability of complex power systems to detect anomalous situations and to react in a timely manner. Surveillance and security technologies are examined extensively in existing literature, but not explicitly in the context of power systems and other critical infrastructures. This motivated us to explore the main technologies applicable in critical infrastructures and to present an evaluation of them based on the perceived opinion of experts. We anticipate that the information we presented will serve as a useful insight for designers, implementers and deployers of new innovative protection systems in future, as well as facilitating interactions amongst the relevant communities. Because of the rapid introduction and use of cyber-physical systems, these communities will involve ICT (information and communication technologies), cyber-security, and the emerging field of resilient systems. However, it is noteworthy that despite the several (technical) advancements in technologies, non-technical risk metrics in critical infrastructures are currently underemphasised. Future work using surveillance and security technologies for protecting critical infrastructures should be a comprehensive approach that introduces monitoring processes in each of the technical layers of these systems (for example the Purdue layers; see [63] or the European Smart Grid Architecture Model (SGAM); see [64]). We also recommend further research on organisational processes, procedures, and peoples' behaviour (see Organisation, Technology, Individual (OTI) viewpoints in [65]), and on monitoring and increasing the resilience of critical infrastructures against cyber-physical threats [66, 67, 68, 69].

Declaration

A. Availability of data and material

The datasets analysed during the current study are not publicly available due to non-disclosure agreements (NDA). Its disclosure to third parties will require written authorisation of all disclosing parties.

B. Funding

This work was supported by the European Union Seventh Framework Programme under grant agreement no. 608090: project HyRiM (Hybrid Risk Management for Utility Providers).
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 764090: project EASY-RES (Enable Ancillary Services bY Renewable Energy Sources).

C. Authors' contributions

AG has made contributions to conception and design, acquisition of data, analysis, interpretation of data and writing the manuscript. BG has made contributions to conception and design, acquisition of data and drafting the manuscript. DH has made contributions to conception and design and has been involved in drafting the manuscript and revising it appropriately. AA has made contributions to conception and design, acquisition of data, interpretation of data and writing the manuscript. HM has made contributions to conception and design and has been involved in drafting the manuscript and revising it appropriately. All authors read and approved the final manuscript.

D. Acknowledgements

Not applicable

E. Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Computing and Communications, Lancaster University, InfoLab21, LA1 4WA Lancaster, UK. [2]Faculty of Computer Science and Mathematics, University of Passau, Passau, Germany.

References

1. Smith, R.: Assault on california power station raises alarm on potential for terrorism. Wall Street Journal **5** (2014)
2. Alert, D.: Cyber-Attack Against Ukrainian Critical Infrastructure. February (2016)
3. Amin, M.: Security challenges for the electricity infrastructure. Computer **35**(4), 8–10 (2002)
4. Rass, S., Alshawish, A., Abid, M.A., Schauer, S., Zhu, Q., De Meer, H.: Physical intrusion games—optimizing surveillance by simulation and game theory. IEEE Access **5**, 8394–8407 (2017)
5. Gong, S., Loy, C.C., Xiang, T.: Security and surveillance, 455–472 (2011)
6. Clarke, R.: Information technology and dataveillance. Communications of the ACM **31**(5), 498–512 (1988)
7. Williams, E., Eyo, B.: Ubiquitous computing: The technology for boundless surveillance
8. Wright, D., Raab, C.D.: Constructing a surveillance impact assessment. Computer Law & Security Review **28**(6), 613–626 (2012)
9. Gouglidis, A., Shirazi, S.N., Simpson, S., Smith, P., Hutchison, D.: A multi-level approach to resilience of critical infrastructures and services. In: Telecommunications (ICT), 2016 23rd International Conference On, pp. 1–5 (2016). IEEE
10. Marinos, L.: Enisa threat landscape 2013: Overview of current and emerging cyber-threats. Heraklion: European Union Agency for Network and Information Security Publishing. doi **10**, 14231 (2013)
11. Bourne, V.: Critical infrastructure readiness report: Holding the line against cyberthreats. The Aspen Institute (2015)
12. Sterbenz, J.P., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schöller, M., Smith, P.: Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks **54**(8), 1245–1265 (2010)
13. Hutchison, D., Kammenhuber, N., Kooij, R., NEC, M.S.: Resilience and survivability for future networking: framework, mechanisms, and experimental evaluation
14. Smith, P., Hutchison, D., Sterbenz, J.P., Schöller, M., Fessi, A., Karaliopoulos, M., Lac, C., Plattner, B.: Network resilience: a systematic approach. IEEE Communications Magazine **49**(7), 88–97 (2011)
15. Jungert, E., Hallberg, N., Wadströmer, N.: A system design for surveillance systems protecting critical infrastructures. Journal of Visual Languages & Computing **25**(6), 650–657 (2014)
16. Sveinsdottir, T., Finn, R., Rodrigues, R., Wadhwa, K., Fritz, F., Kreissl, R., Hert, A.T., van Brakel, R.: Taxonomy of security products, systems and services
17. van Rest, J.: Surveillance use cases: focus on video analytics. Technical report, European Commission (2015)
18. Commission, E.: European programme for critical infrastructure protection, ol. 786 final, p. 13,. EC, Brussels **17** (2006)
19. Automation, R.: Converged Plantwide Ethernet (CPwE) Design and Implementation Guide.". Citeseer (2011)
20. Carlson, R.: Sandia scada program high-security scada ldrd final report. SANDIA Report SAND **729**, 2002 (2002)
21. Dawson, R., Boyd, C., Dawson, E., Nieto, J.M.G.: Skma: a key management architecture for scada systems. In: Proceedings of the 2006 Australasian Workshops on Grid Computing and e-research-Volume 54, pp. 183–192 (2006). Australian Computer Society, Inc.
22. Coen, v.G., Hauke, V., Sebastian, H., Olexander, Y.: Surveille Deliverable 2.1: Survey of surveillance technologies, including their specific identification for further work. Surveille Project, European Commission, Bruxelles (2012)
23. Bellanova, R., Friedewald, M.: Deliverable 1.1: Smart surveillance–state of the art. SAPIENT. FP7 Sapient Project, Brussels. http://www. sapientproject. eu/docs D **1** (2011)

24. Guelke, J., Sorell, T., Hadjimatheou, K., Scheinin, M., Andrew, J., Lavapuro, J., Ojanen, T., Grazia Porcedda, M., Vermeulen, M., McNeill, B., et al.: Surveille deliverable 2.6: Matrix of surveillance technologies. Seventh Framework Programme. Surveillance: Ethical Issues, Legal Limitations, and Efficiency, FP7-SEC-2011-284725 (2013)
25. Gulzar, N., Abbasi, B., Wu, E., Ozbal, A., Yan, W.: In: Atrey, P.K., Kankanhalli, M.S., Cavallaro, A. (eds.) Surveillance Privacy Protection, pp. 83–105. Springer, Berlin, Heidelberg (2013). doi:10.1007/978-3-642-41512-8_5. https://doi.org/10.1007/978-3-642-41512-8_5
26. Thalmann, D., Salamin, P., Ott, R., Gutiérrez, M., Vexo, F.: Advanced mixed reality technologies for surveillance and risk prevention applications. In: International Symposium on Computer and Information Sciences, pp. 13–23 (2006). Springer
27. Hampapur, A., Brown, L., Connell, J., Pankanti, S., Senior, A., Tian, Y.: Smart surveillance: applications, technologies and implications. In: Information, Communications and Signal Processing, 2003 and Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint Conference of the Fourth International Conference On, vol. 2, pp. 1133–1138 (2003). IEEE
28. Senior, A.: An introduction to automatic video surveillance, 1–9 (2009)
29. ULD, E.S., ULD, M.H., Sterbik-Lamina, J.: D 3.1–report on surveillance technology and privacy enhancing design
30. Weber, K.: The next step: privacy invasions by biometrics and ict implants. Ubiquity **2006**(November), 4 (2006)
31. Mueller, M., Kuehn, A.: Einstein on the breach: Surveillance technology, cybersecurity and organizational change. In: 12th Workshop on the Economics of Information Security (WEIS 2013), Georgetown University, Washington, DC June, pp. 11–12 (2013)
32. Nguyen, D.H., Marcu, G., Hayes, G.R., Truong, K.N., Scott, J., Langheinrich, M., Roduner, C.: Encountering sensecam: personal recording technologies in everyday life. In: Proceedings of the 11th International Conference on Ubiquitous Computing, pp. 165–174 (2009). ACM
33. Sutor, S., Reda, R.: Multi sensor technologies augmenting video surveillance: Security and data fusion aspects. In: Computer and Information Sciences, 2008. ISCIS'08. 23rd International Symposium On, pp. 1–4 (2008). IEEE
34. Meggitt, D., Roderick, D., Cooke, K.: Advanced technologies for undersea surveillance of modern threats. In: OCEANS'99 MTS/IEEE. Riding the Crest Into the 21st Century, vol. 1, pp. 289–294 (1999). IEEE
35. Norris, C., Lyon, D.: Surveillance as social sorting: Privacy, risk, and digital discrimination (2003)
36. Brassil, J.: In: Senior, A. (ed.) Technical Challenges in Location-Aware Video Surveillance Privacy, pp. 91–113. Springer, London (2009). doi:10.1007/978-1-84882-301-3_6. https://doi.org/10.1007/978-1-84882-301-3_6
37. Hu, W., Tan, T., Wang, L., Maybank, S.: A survey on visual surveillance of object motion and behaviors. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) **34**(3), 334–352 (2004)
38. Hu, W.-F., Chen, Y.-S., Hsieh, J.-W.: Vehicle occlusion identification system by perceptive roadway modeling. In: MVA, pp. 392–397 (2005)
39. Mordini, E., Petrini, C.: Ethical and social implications of biometric identification technology. Annali dell'Istituto superiore di sanita **43**(1), 5–11 (2007)
40. Nwatu, G.U.: Biometrics technology: Understanding dynamics influencing adoption for control of identification deception within nigeria (2011)
41. Ross, A., Jain, A.K.: Multimodal biometrics: An overview. In: Signal Processing Conference, 2004 12th European, pp. 1221–1224 (2004). IEEE
42. nidirect: Using ePassport gates at airport border control (2014). https://www.nidirect.gov.uk/articles/using-epassport-gates-airport-border-control
43. FBI: Combined DNA Index System (CODIS) (2011). https://www.fbi.gov/services/laboratory/biometric-analysis/codis
44. FBI: Combined DNA Index System Operational and Laboratory Vulnerabilities (2006). https://oig.justice.gov/reports/FBI/a0632/final.pdf
45. TheGuardian: NSA collecting phone records of millions of Verizon customers daily (2013). https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
46. TheGuardian: Snowden leak: governments' hostile reaction fuelled public's distrust of spies (2015). https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies
47. Hightower, J., Borriello, G.: Location systems for ubiquitous computing. Computer **34**(8), 57–66 (2001)
48. Degli Esposti, S.: When big data meets dataveillance: The hidden side of analytics. Surveillance & Society **12**(2), 209 (2014)
49. Scarfone, K., Mell, P.: Guide to intrusion detection and prevention systems (idps). NIST special publication **800**(2007), 94 (2007)
50. Bonifati, A., Cattaneo, F., Ceri, S., Fuggetta, A., Paraboschi, S., *et al.*: Designing data marts for data warehouses. ACM transactions on software engineering and methodology **10**(4), 452–483 (2001)
51. Mawilmada, P.K.: Impact of a data warehouse model for improved decision-making process in healthcare. PhD thesis, Queensland University of Technology (2011)
52. Rachana, S., Guruprasad, H.: Virtual machine introspection. Compusoft **3**(6), 860 (2014)
53. Wigan, M.R., Clarke, R.: Big data's big unintended consequences. Computer **46**(6), 46–53 (2013)
54. Clarke, R.: Profiling: A hidden challenge to the regulation of data surveillance. JL & Inf. Sci. **4**, 403 (1993)
55. Antonello, R., Fernandes, S., Kamienski, C., Sadok, D., Kelner, J., GóDor, I., Szabó, G., Westholm, T.: Deep packet inspection tools and techniques in commodity platforms: Challenges and trends. Journal of Network and Computer Applications **35**(6), 1863–1878 (2012)
56. Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., Vainio, N., Myllymäki, P.: Long-term effects of ubiquitous surveillance in the home. In: Proceedings of the 2012 ACM Conference on

Ubiquitous Computing, pp. 41–50 (2012). ACM
57. Greenfield, A.: Everyware: The dawning age of ubiquitous computing. Voices That Matter. Pearson Education, Berkeley, CA 94710 (2010). https://books.google.co.uk/books?id=noMNgMcZvL0C
58. Uteck, A.: Ubiquitous computing and spatial privacy. Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, 83–101 (2009)
59. Dodge, M., Batty, M., Kitchin, R.: No longer lost in the crowd: Prospects of continuous geosurveillance. In: Association of American Geographers Annual Conference (2004)
60. Bankston, K.S., Soltani, A.: Tiny constables and the cost of surveillance: Making cents out of united states v. jones. Yale LJF **123**, 335 (2013)
61. Ali, A., Zhiyuan, S., Antonios, G., Syed, A.A.N., Paolo, G., Massimiliano, T.: HyRiM Deliverable 4.3: How to Enhance Perimeter Security Using New Surveillance Technologies (2017). https://hyrim.net/wp-content/uploads/2017/12/HyRiM-D4.3-How-to-Enhance-Perimeter-Security-using-new-Surveillance-Technologies.pdf
62. Alshawish, A., Amine Abid, M., de Meer, H., Schauer, S., König, S., Gouglidis, A., Hutchison, D.: G-dps: A game-theoretical decision-making framework for physical surveillance games (2018)
63. Obregon, L.: Secure architecture for industrial control systems. SANS Institute InfoSec Reading Room (2015)
64. Uslar, M., Rosinger, C., Schlegel, S.: Security by design for the smart grid: Combining the sgam and nistir 7628. In: Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International, pp. 110–115 (2014). IEEE
65. Gouglidis, A., Green, B., Busby, J., Rouncefield, M., Hutchison, D., Schauer, S.: Threat awareness for critical infrastructures resilience. In: Resilient Networks Design and Modeling (RNDM), 2016 8th International Workshop On, pp. 196–202 (2016). IEEE
66. Esposito, C., Gouglidis, A., Hutchison, D., Gurtov, A., Helvik, B., Heegaard, P., Rizzo, G., Rak, J.: On the disaster resiliency within the context of 5g networks: The recodis experience (2018)
67. Gouglidis, A., König, S., Green, B., Rossegger, K., Hutchison, D.: In: Rass, S., Schauer, S. (eds.) Protecting Water Utility Networks from Advanced Persistent Threats: A Case Study, pp. 313–333. Springer, Cham (2018). doi:10.1007/978-3-319-75268-6_13. https://doi.org/10.1007/978-3-319-75268-6_13
68. Gouglidis, A., Hu, V.C., Busby, J.S., Hutchison, D.: Verification of resilience policies that assist attribute based access control. In: Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control, pp. 43–52 (2017). ACM
69. Machuca, C.M., Secci, S., Vizarreta, P., Kuipers, F., Gouglidis, A., Hutchison, D., Jouet, S., Pezaros, D., Elmokashfi, A., Heegaard, P., *et al.*: Technology-related disasters: A survey towards disaster-resilient software defined networks. In: Resilient Networks Design and Modeling (RNDM), 2016 8th International Workshop On, pp. 35–42 (2016). IEEE
70. Mayer, P.: Guidelines for writing a review article. Zurich-Basel: Plant Science Center. Dostupné z http://www. plantscience. ethz. ch/education/Masters/courses/Scientific_Writing (2009)
71. Qiu, D., Li, B., Ji, S., Leung, H.: Regression testing of web service: a systematic mapping study. ACM Computing Surveys (CSUR) **47**(2), 21 (2015)
72. Budgen, D., Brereton, P.: Performing systematic literature reviews in software engineering. In: Proceedings of the 28th International Conference on Software Engineering, pp. 1051–1052 (2006). ACM
73. Such, J.M., Gouglidis, A., Knowles, W., Misra, G., Rashid, A.: Information assurance techniques: Perceived cost effectiveness. Computers & Security **60**, 117–133 (2016)

Appendix A

A systematic literature review of surveillance technologies was conducted in this paper to identify and analyse various individual projects and prior research work. This review was designed to provide a wide overview of a research area, to classify information and provide comparative information. We decided to perform this type of review since our goal is to overview state-of-the-art technological trends and best practices in the surveillance area. Specifically, in order to accomplish this objective, we conduct a systematic review similar to that in [70].

Research questions

The specification of a set of questions to be answered is considered to be extremely important to be able to conduct a systematic review. Therefore, we have created two different sets of question categories, viz. general questions (GQ), and focused questions (FQ). In Table 5, we list the set of defined research questions per category. The set of general questions is concerned with the identification of general trends of surveillance technologies. This type of questions will help to perform a landscaping with regard to current surveillance technologies. GQ1 is concerned with the type of surveillance technologies that are examined or proposed. This will result in extracting adequate information about the different technologies used. GQ2 identifies which surveillance technologies are used in a certain kind of surveillance area. This might be an important factor since it may lead to identify which technologies are best suited for application in utility networks. Lastly, GQ3 questions the challenges of enforcing the identified surveillance technologies. This will eventually unveil the main issues that the majority of surveillance technologies encounter and provide thoughts for future consideration.

Focused questions address the classification of surveillance technologies in several dimensions, here security, privacy, and usability. FQ1 focuses on technologies that are capable of improving the security in various areas. FQ2 concentrates on the level of privacy infringement imposed by the application of any type of surveillance technologies. Additionally, ways of protecting the privacy of people are also examined. Finally, FQ3 explores the usability of the identified technologies within certain areas.

Search Strategy

Finding a complete set of primary studies is the next step. As stated in [71], these studies should have a relation with the research questions, and also ensure that are not biased. This would require following a search strategy, which may include the construction of an appropriate set of keywords, which will eventually define the scope of the search strategy.

Construction of search keywords

In order to achieve an accurate search result, it is required to perform a search using an appropriate combination of keywords, which are strongly related to the topic under research. To frame research questions a set of criteria can be used. These criteria can lead to the refinement and optimisation of the group of keywords, and thus, provide guides for the selection of primary studies. Some of these criteria consist of population, intervention, comparison, outcome and context [72]. Specifically, we are mostly interested in populations and intervention. This is because, as stated in [71], 'populations' may involve terms related to standards and technologies, while 'intervention' addresses specific issues in technologies. Conducting search questions using individual surveillance controls, e.g., camera, sensors, etc., does not result in retrieving the desired outcome. Therefore, in order to restrict the results, we defined context-based search keywords. We consider as context the keyword 'surveillance'. Again, this has to further be refined by a population keyword. Therefore, we set 'technologies' as our population keyword. Hence, the final keyword set is: surveillance AND technologies, with AND being the usual Boolean operator.

Sources of information

The literature review was carried out on manuscripts that were obtained from several on-line electronic databases, and by performing search queries using our defined keyword set. To cover the majority of existing information, information retrieval was conducted using eight different on-line databases. Table 6 lists the set of selected electronic libraries. The selected databases are known to cover the most relevant journals, conference and workshop publications within the area of computing and engineering. The initial search resulted in 862 potentially relevant papers on surveillance technologies.

The initial set of documents was filtered in order to exclude irrelevant studies from our survey, and thus, to include the most representative studies for that. The process of identifying the primary studies included an initial filtration of the gathered information by title. This included looking, once again, for representative keywords, as stated before. The second step resulted in 150 studies (i.e., reduced by 82.59%), which were further collated, to exclude duplicates, and examined for their on-line availability. The latter process resulted in 116 documents (i.e., reduced by 22.66%). The next step included the filtering of the studies based on the information included in their abstract. Documents not referring to surveillance systems (e.g., surveillance of medical deceases) were excluded, and thus, resulting in 60 individual studies (i.e., reduced by 48.27%). The final step included the reading of the full paper, and exclusion of these that did not provide adequate information with regard to the defined research questions. This last step led to the identification of 16 documents (i.e., reduced by 73.33%) that represented the main source of information for the overview study of surveillance technologies.

In Table 7, we list the studies that have been identified through the previous data gathering process. Specifically, we assign an identification code (ID) to each study document in column one (S1 – S15); we refer to the researchers that performed the primary study in column two; and finally, we provide the title of the study document in column three.

Table 5 Research questions.

Reference	Question
General questions	
GQ1	Which surveillance technologies are proposed or examined?
GQ2	What application areas are proposed or examined for surveillance technologies?
GQ3	What are the challenges in surveillance technologies?
Focused Questions	
FQ1	Which technologies are able to improve the level of security offered by surveillance technologies?
FQ2	Which privacy implications of surveillance technologies are examined?
FQ3	Which technologies are examined to improve the usability of surveillance technologies within certain areas?

Table 6 Selected electronic databases.

Electronic database	Website
ACM Digital Library	http://dl.acm.org/
CiteSeerX	http://citeseerx.ist.psu.edu/index
CORDIS	http://cordis.europa.eu/projects/home_en.html
Google Scholar	https://scholar.google.co.uk/
IEEE Xplore Digital Library	http://ieeexplore.ieee.org/Xplore/home.jsp
ScienceDirect Library	http://www.sciencedirect.com/
Scopus	http://www.scopus.com/
SpringerLink	http://link.springer.com/

Table 7 List of primary studies.

ID	Primary study	Title
S1	[Gulijk et al., 2012]	Survey of surveillance technologies, including their specific identification for further work
S2	[Bellanova & Friedewald, 2011]	Smart Surveillance – State of the Art
S3	[Guelke et al., 2013]	Matrix of Surveillance Technologies
S4	[Schlehahn et al., 2013]	Report on surveillance technology and privacy enhancing design
S5	[Nguyen et al., 2009]	Encountering SenseCam: Personal Recording Technologies in Everyday Life
S6	[Weber, 2006]	The Next Step: Privacy Invasions by Biometrics and ICT Implants
S7	[Thalmann, Salamin, Ott, Gutiérrez, & Vexo, 2006]	Advanced Mixed Reality Technologies for Surveillance and Risk Prevention Applications
S8	[Hampapur et al., 2003]	Smart Surveillance: Applications, Technologies and Implications
S9	[Williams & Eyo]	Ubiquitous Computing: The Technology for Boundless Surveillance
S10	[Mueller & Kuehn, 2013]	Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change
S11	[Sutor & Reda, 2008]	Multi Sensor Technologies Augmenting Video Surveillance: Security and Data Fusion Aspects
S12	[Senior, 2009]	An Introduction to Automatic Video Surveillance
S13	[Meggitt, Roderick, & Cooke, 1999]	Advanced Technologies for Undersea Surveillance of Modern Threats
S14	[Gulzar, Abbasi, Wu, Ozbal, & Yan, 2013]	Surveillance Privacy Protection
S15	[Gong, Loy, & Xiang, 2011]	Security and Surveillance

Quality assessment

Since the assessment of primary studies is critical, we adopted a set of quality criteria, as defined in [71], to perform an appropriate assessment. In particular, these criteria are expressed with the following list of quality assessment (QA) questions:

QA1: Is there a clear statement about the aim of the research?
QA2: Is there an adequate description of the research context?
QA3: Is there a review about related work of problem?
QA4: Is the conclusion related to the aim and purpose of research defined?
QA5: Is there a clear statement of findings?
QA6: Does the study recommend further research?

Table 8 depicts the result of our analysis after applying the defined set of quality assessment criteria to the list of identified primary studies. This indicated that not all of our defined criteria are achieved by all primary studies; however, we have decided not to eliminate them since not being able to fulfil all the criteria in this study does not affect the extraction of required information. Specifically, we use the 'X' symbol (i.e., 'yes') to indicate that a study fulfils a criterion and left as blank (meaning 'no') to indicate non-fulfilment of one of the criteria.

Table 8 Quality assessment for primary studies.

Primary study	QA1	QA2	QA3	QA4	QA5	QA6
S1	X	X				X
S2	X	X	X	X		
S3	X	X			X	
S4	X	X		X	X	
S5	X	X	X	X	X	X
S6	X			X		
S7	X	X		X	X	
S8	X	X	X	X	X	
S9	X				X	
S10	X	X		X	X	
S11	X			X		X
S12	X	X		X		
S13	X	X		X	X	
S14	X	X	X		X	
S15	X	X	X	X		X

Data extraction

With regard to data extraction, this was done on the basis of the collected study documents. Specifically, in Table 9, we illustrate the source of information for each of the defined type of questions (i.e., generic and focused).

Table 9 Data extraction from primary studies.

Primary study	GQ1	GQ2	GQ3	FQ1	FQ2	FQ3
S1	X			X		
S2	X	X	X	X	X	
S3	X	X			X	X
S4	X	X	X			
S5	X	X			X	
S6	X	X			X	
S7	X			X		
S8	X	X	X	X	X	
S9	X		X		X	
S10	X	X		X	X	
S11	X	X	X	X		
S12	X				X	
S13	X	X	X			
S14	X	X			X	
S15	X	X	X	X		

Appendix B

Experts operating in utility networks provided the data for evaluating the metrics. In all cases, the level of confidence with regard to the given information is taken into consideration. In more detail, we performed a mapping of qualitative values to quantitative ones, which we have developed and applied in [73].

The applied mappings are provided in the following:

- Confidence = {(high = 1), (medium = 0.5), (low = 0.1)}.
- Security = {(excellent = 1), (very good = 0.8), (good = 0.6), (fair = 0.4), (poor = 0.2)}.
- Privacy = {(excellent = 1), (very good = 0.8), (good = 0.6), (fair = 0.4), (poor = 0.2)}.
- Usability = {(excellent = 1), (very good = 0.8), (good = 0.6), (fair = 0.4), (poor = 0.2)}.
- Effectiveness = {(excellent = 1), (very good = 0.8), (good = 0.6), (fair = 0.4), (poor = 0.2)}.
- Cost = {(extremely expensive = 1), (very expensive = 0.8), (expensive = 0.6), (moderate = 0.4), (cheap = 0.2)}.

Based on these sets, the formula used for calculating the cost-effectiveness of a security technology (ST) is:

$$Cost\_Effectiveness_{ST} = Effectiveness_{ST} \times (1 - Cost_{ST}) \tag{1}$$

In formula 1 it is required to calculate the frequency of variables values (i.e., obtains count on a single variable's values) to compute average effectiveness (i.e., $Effectiveness_{ST}$). This is expressed in the range of [0, 1]. Likewise, we calculate the average cost of a technology. Since the cost of each technology is considered to be inversely proportional to its overall cost effectiveness, we subtract $Cost_{ST}$ from 1 (all values are expressed in the range of [0, 1]). Following, we use VP to refer to 'Valid Percentage', i.e., a percentage that does not include missing cases. Specifically, we have that:

$$VP_{value} = (ValueOccurrences)/(Totalnumberofvalues), VPvalue \in [0, 1] \tag{2}$$

Additionally, it holds that:

$$Confidence_{ST} = (1 \times VP_{high} + 0.5 \times VP_{medium} + 0.1 \times VP_{low}) \tag{3}$$

$$\begin{aligned} Effectiveness_{ST} = Confidence_{ST} \times (1 \times VP_{excellent} + 0.8 \times VP_{verygood} + \\ 0.6 \times VP_{good} + 0.4 \times VP_{fair} + 0.2 \times VP_{poor}) \end{aligned} \tag{4}$$

And,

$$\begin{aligned} Cost_{ST} = Confidence_{ST} \times (1 \times VP_{extremelyexpensive} + 0.8 \times VP_{veryexpensive} + \\ 0.6 \times VP_{expensive} + 0.4 \times VP_{moderate} + 0.2 \times VP_{cheap}) \end{aligned} \tag{5}$$

Appendix C

The information in Table 10 provides detailed information about the computed values on experts' perception, i.e., before and after applying confidence to experts' opinion.

Table 10 Perception of experts in utility networks.

		Security	Privacy	Usability	Effectiveness	Cost	Confidence
Visual surveillance	Calculated value (Cv.)	0.7000	0.6667	0.6333	0.4667	0.3333	0.8333
	Cv. * Confidence	0.5833	0.5556	0.5278	0.3889	0.2778	
	Cost Effectiveness	0.2809					
Biometrics	Calculated value (Cv.)	0.7000	0.5000	0.6000	0.6000	0.3000	1.0000
	Cv. * Confidence	0.7000	0.5000	0.6000	0.6000	0.3000	
	Cost Effectiveness	0.4200					
Communication surveillance	Calculated value (Cv.)	0.5500	0.4750	0.6000	0.4250	0.4500	0.8750
	Cv. * Confidence	0.4813	0.4156	0.5250	0.3719	0.3938	
	Cost Effectiveness	0.2254					
Location tracking	Calculated value (Cv.)	0.7000	0.7500	0.6000	0.4000	0.4500	1.0000
	Cv. * Confidence	0.7000	0.7500	0.6000	0.4000	0.4500	
	Cost Effectiveness	0.2200					
Dataveillance	Calculated value (Cv.)	0.5778	0.5111	0.5111	0.5333	0.5333	0.7778
	Cv. * Confidence	0.4494	0.3975	0.3975	0.4148	0.4148	
	Cost Effectiveness	0.2427					
Ubiquitous surveillance	Calculated value (Cv.)	0.4500	0.6000	0.5500	0.5000	0.3000	0.4000
	Cv. * Confidence	0.1800	0.2400	0.2200	0.2000	0.1200	
	Cost Effectiveness	0.1760					